

ETAPPE 3

Datenschutz im KI-Arbeitsprozess

Wie du Kontext, Dateien und mehrere KI-Schritte sicher gestaltest

... und warum Uster aktuell noch keine Agenten baut

Pfad 3: Gestalten · Expert:innen

Rückblick: von Etappe 1 und 2 zu heute

Was wir schon können – und was heute dazukommt.



DARUM GEHT ES HEUTE

Wir betrachten KI-Nutzung nicht als einzelnen Prompt, sondern als durchgängigen Datenfluss – von der Quelle über den Arbeitsordner bis zum Zwischenergebnis.

Agenda

Vier Fragen führen uns durch diesen Lernimpuls

1

Wo stehen wir?

KI-Reifegrade – wo die Stadt Uster heute steht

2

Wo arbeiten wir?

Die Datenreise und die richtige Umgebung: Varios

3

Was geben wir ein?

Die KI-Ampel, das Mosaik-Prinzip und der Gelb-Check

4

Was tun wir konkret?

Der Datenblick – dein Vorgehen in der Praxis

Lernziele

Nach diesem Lernimpuls kannst du ...



den Datenfluss durch den ganzen Arbeitsprozess verfolgen – nicht nur den einzelnen Prompt.



Inhalt und Umgebung getrennt prüfen – mit KI-Ampel und Gelb-Check.



typische Datenlecks in Dateien erkennen – Restname, Metadaten, veraltete Quelle, Prompt Injection.



rote Fälle mit der Platzhalter-Methode sicher bearbeiten: vorbereiten → mit KI → lokal ergänzen.

Wo Uster heute steht

① WO STEHEN WIR?

... und warum komplexe Lösungen wie Assistenten, RAGs und Agenten noch etwas warten müssen.

► USTER STEHT HEUTE HIER · ÜBERGANG RF 1 → 2

		RF 1	RF 2	RF 3	RF 4
ORGANISATION	USER	Bewusstsein schaffen – Erste KI-Tools im Einsatz – Keine übergreifende Strategie – Nicht freigegebene Tools (Schatten-KI)	Strukturen etablieren – Klare Governance – Sichere Plattform – Systematische Befähigung	Prozesse optimieren – KI in allen Prozessen – Messbare Erfolge – Kontinuierliche Optimierung	Innovation vorantreiben – KI als DNA der Organisation – Strategischer Wettbewerbsvorteil
		Basic User – Sichere Alltagseffizienz – Basic-Prompting – Zusammenfassungen & E-Mails	Power User – Qualität & Komplexität – Advanced-Prompting – Assistenten werden genutzt	Koordinatoren – Bauen & Befähigen – Use Case Engineering – Teams & Best Practices	IT & Spezialisten – Plattform betreiben – Varios-Administration – Support

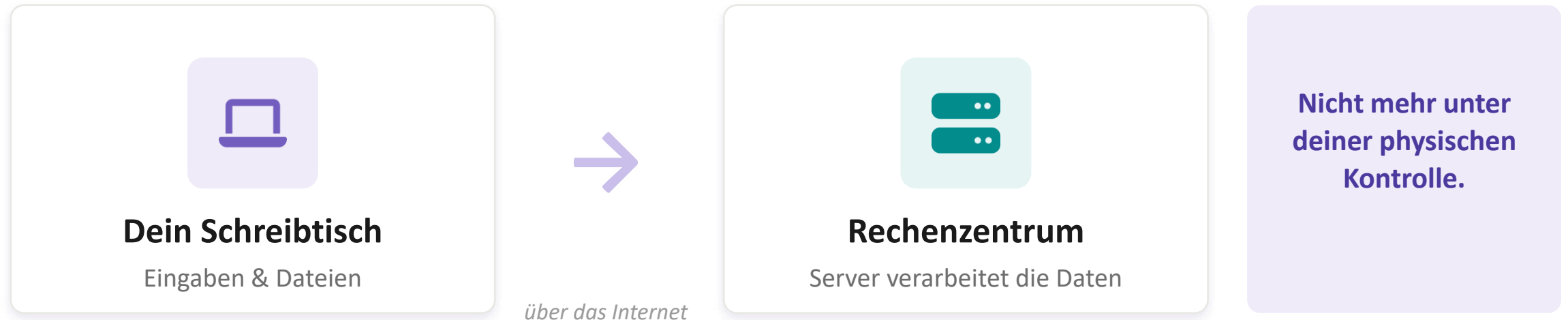
WAS DAS HEISST

Erst wenn die Grundlagen von Reifegrad 2 stabil sind, entstehen gemeinsame Assistenten, Wissensarchive und Agenten – verantwortungsvoll, nicht sofort. Eure Ideen sind dafür schon willkommen

Die Reise der Daten

② WO ARBEITEN WIR?

Was technisch passiert, wenn du auf ‹Senden› klickst.



MERKSATZ

Sobald du auf ‹Senden› klickst, verlässt deine Eingabe den Schreibtisch. Deshalb ist entscheidend, wohin sie geht – und darum brauchen wir eine freigegebene Umgebung.

Postkarte, Briefumschlag und Aktenkoffer

② WO ARBEITEN WIR?

Warum Arbeitsinhalte in Varios gehören.

OFFEN



Postkarte

Offene oder private KI-Tools – jeder könnte mitlesen. Das ist Schatten-KI.

GESCHÜTZT



Briefumschlag

Geschäftliche Umgebung mit Schutzvereinbarung – aber nicht für die Stadt freigegeben.

FREIGEgeben



Aktenkoffer = Varios

Der besonders geschützte, geregelte Rahmen – für städtische Arbeit der einzige richtige Ort

SCHATTEN-KI VS. VARIOS

Schatten-KI heisst: nicht freigegebene oder private KI-Tools für Arbeitsinhalte nutzen. Für die Stadt Uster ist Varios der einzige richtige Ort – geschützt, geregelt und freigegeben.

Das Sicherheitsnetz: DLP

③ WAS GEBEN WIR EIN?

Ein technisches Netz – aber kein Ersatz für den eigenen Blick.



DLP-HINWEIS

Mögliche Personendaten erkannt

«... Antwort an Marc Müller, Seestr...»

Bitte vor dem Senden prüfen.

Erkennt Muster

von Namen, Adressen und Nummern – und warnt vor dem Senden.

Kennt den Kontext nicht

das Mosaik hinter den Daten erkennt es nicht.

MERKSATZ

Varios unterstützt euch technisch – aber es kann den Kontext nicht vollständig beurteilen. Deshalb braucht es jetzt ein menschliches Vorgehen: den Datenblick.

Die KI-Ampel

③ WAS GEBEN WIR EIN?

Vor jeder Eingabe: Ist der Inhalt grün, gelb oder rot?



Grün

öffentlich – jeder darf es wissen

BEISPIEL

Veröffentlichte Medienmitteilung



Gelb

intern, ohne Personendaten – nur
Varios

BEISPIEL

Interne Vorlage ohne Namen



Rot

persönlich oder vertraulich – nie im
Original

BEISPIEL

Name · Krankheitsdaten · Fallnummer

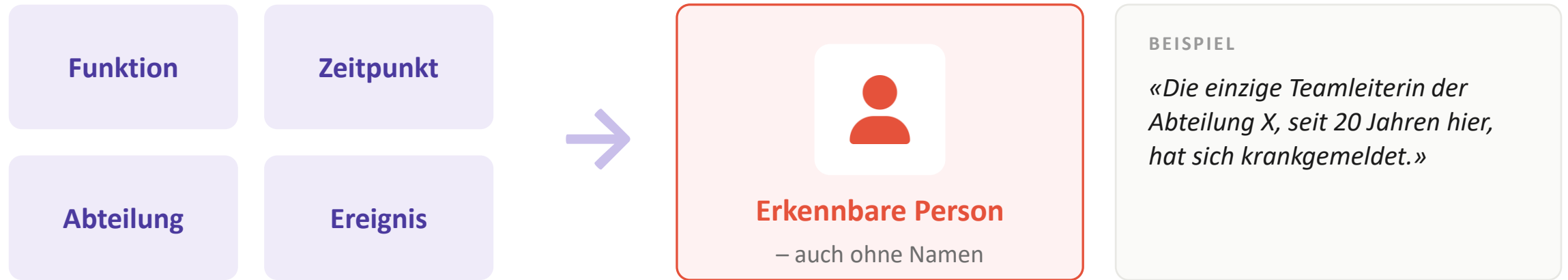
FAUSTREGEL

**Persönlich oder vertraulich? → Rot · nur intern, ohne Personendaten? → Gelb · öffentlich? → Grün.
Und wichtig: Rot heisst nie im Original – ausser es gibt einen freigegebenen, erlaubten Prozess.**

Das Mosaik-Prinzip

Indirekte Erkennbarkeit – auch ohne Namen.

③ WAS GEBEN WIR EIN?



MERKSATZ

Ein Text ist erst sicher, wenn niemand aus den Puzzleteilen ein Bild zusammensetzen kann. Diesen Blick brauchen wir gleich beim Gelb-Check.

Der Gelb-Check

③ WAS GEBEN WIR EIN?

Wenn die Ampel nicht sofort reicht – die Grenzfälle klären.

1 Ist eine Person direkt oder indirekt erkennbar? (Mosaik!)

2 Geht es um sensible Themen – Gesundheit, Finanzen, Vertrauliches?

3 Ist die Information nur für einen kleinen Kreis bestimmt?

SO ENTSCHIEDEST DU

Ein «Ja» → behandle den Fall als Rot. Unsicher? Kurz stoppen und nachfragen – eine kurze Frage ist besser als ein ungutes Gefühl.

Drei Anonymisierungs-Werkzeuge

④ WAS TUN WIR KONKRET?

«Die KI muss nie erfahren, um wen es geht — nur worum.»

Anonymisieren

Alle Identifier raus.

Namen, Adressen, Geburtsdaten, eindeutige Merkmale entfernen — so dass niemand mehr rückschliessen kann.

Beispiel

Maria Müller, Bahnhofstr. 12 → eine Bürgerin

Pseudonymisieren

Platzhalter setzen.

Identifier durch Platzhalter ersetzen — die Zuordnung behältst du extern. Aber: pseudonymisiert ist nicht automatisch anonym — bei möglicher Zuordnung oder erkennbarem Kontext bleibt Vorsicht nötig.

Beispiel

Maria Müller → Person A

Aggregieren

Einzelfall zur Gruppe machen.

Statt einer Person eine Klasse, statt einem Ereignis ein Muster. Nur sicher, wenn keine Einzelperson oder Kleinstgruppe mehr erkennbar ist.

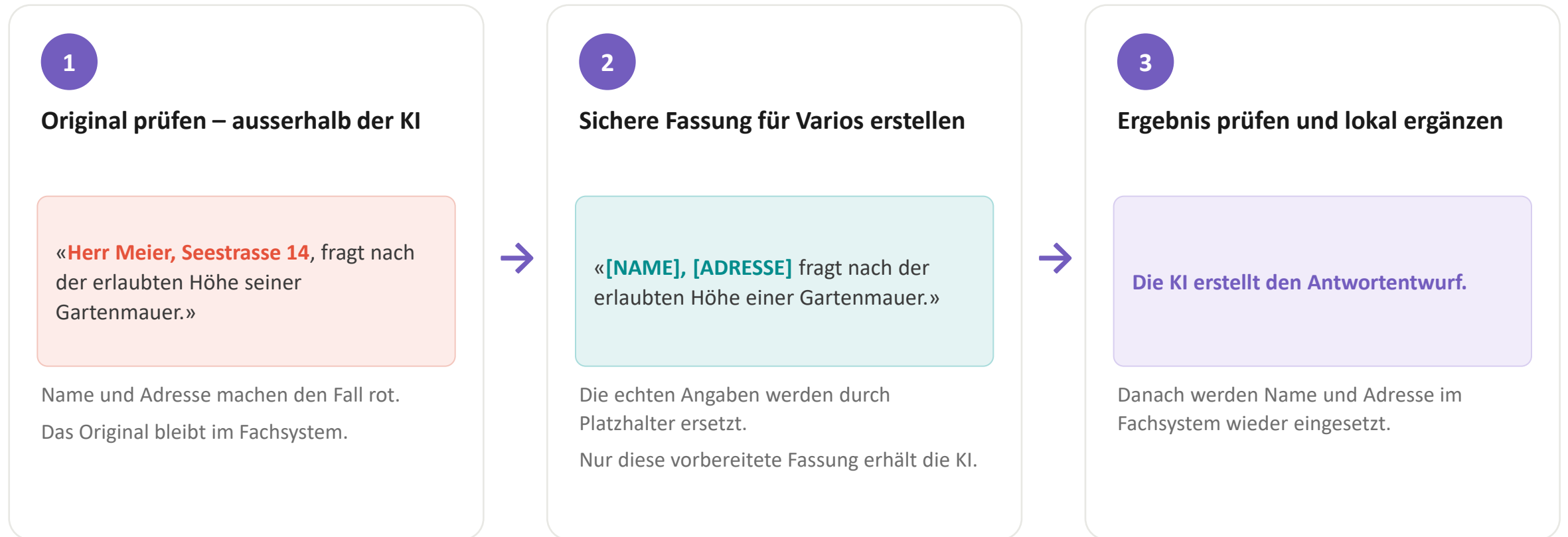
Beispiel

Maria Müllers
Beschwerde → typische
Bürgeranfrage zum
Thema X

Praxisfall: Pseudonymisieren mit Platzhaltern

④ WAS TUN WIR KONKRET?

So wird aus einem roten Originalfall ein sicherer Auftrag für die KI.



MERKSATZ Die KI muss wissen, worum es geht – aber nicht, um wen.

Die vier Leck-Typen bei Dateien

④ WAS TUN WIR KONKRET?

Unser Fall: Herr Meier schreibt uns wegen der Mauerhöhe.



Restname

Ein echter Name steckt noch in der Mustervorlage.

①



Metadaten

Kommentare & Änderungsverlauf verraten mehr, als du siehst.

②



Veraltete Quelle

Falsche Version → die KI übernimmt alte Fehler als Wahrheit.

③



Prompt Injection

Fremde Datei mit versteckten Befehlen an die KI.

④

Vor jedem Upload: Ist die Datei sauber – und braucht die KI sie zwingend? Genau diese vier Lecks sucht ihr gleich in der Gruppenarbeit.

Fünf Spielregeln für den Alltag

- 1 In der richtigen Umgebung arbeiten**
- 2 Inhalt vor dem Senden prüfen**
- 3 Nur so viele Informationen wie nötig verwenden**
- 4 Rote Daten zuerst sicher vorbereiten**
- 5 Ergebnis prüfen und Originalangaben lokal ergänzen**

ABSCHLUSS

Nicht nur der Prompt zählt – entscheidend ist der gesamte Datenfluss durch den Arbeitsprozess.

Prüfen · reduzieren · lokal ergänzen · im Zweifel fragen